National Institutes of Health
Warren Grant Magnuson Clinical Center
Nursing and Patient Care Services

Policy: Administrative Electronic Information: Access, Use and Security

Nursing and Patient Care Service employees have access to a variety of electronic information systems. The type and extent of access is determined by the employee's position description. Supervisors may grant additional access if the employee's job requirements extend beyond those of the standard position description. Examples of electronic information access may include but are not limited to the local area network (LAN), its application and software data, the Automated Nurse Staffing and Office System, (ANSOS), the Integrated Time and Attendance System (ITAS), the electronic mail system, (Outlook), and the Internet. All these uses are intended for official and authorized purposes only. All individuals who use NIH computer resources must, by law, complete the NIH Computer Security Awareness Training annually.

Purpose: To protect confidentiality of information and to identify the process for the use of electronic information and access.

Addendum:

Appendix (1) Management of Access Codes
Appendix (2) Guidelines for the Use of Electronic Information and Resources

Resources:

1. PHS IRM Manual Chapter: Relationship of E-Mail to Records Management and the Privacy Act of 1974
2. Privacy Act, 1974
3. Facsimile Transmission of Individually Identifiable, Confidential Medical Record Information Maintained Under the Privacy Act, April 27, 1998.
4. HHS IRM Policy for Personal Use of Information Technology Resource; Project: HHS IRM Policy Document Number HHS IRM-2000-2003; Jan 8, 2001.
5. HHS IRM Policy for Policy for IT Security for Remote Access; Project HS IRM Policy Document Number: HHS IRM 2000-2005, January 8, 2001
6. NIH Computer Security Awareness Training (http://irtsectraining.nih.gov/)

Approved:

//s//
Clare Hastings, RN, PhD
Chief, Nursing & Patient Care Service

Formulated: **7/93**
Implemented: **7/93**
Revised: **5/95, 7/99, 10/03**

Electronic Information: Access, Use and Security

Appendix (1) Management of Access Codes

Request for Code Access originate from the Recruitment Office at the time of orientation. Documents used in this process are:

- Assignment and Termination of Electronic Access Code Form
- Pyxis Medstation and Supply Station User Contracts
- Certificate of completion of NIH Computer Security Awareness Course

Request for Code Termination at the time of resignation or transfer to another department originates from the Nurse Manager, who sends a Personal Action Request (PAR) to the office of the Service Chief.

- Program Support Assistant puts the termination date in ANSOS and fills out the form to terminate access.
- The Administrative Officer signs the termination form and forwards the paperwork to the appropriate departments.

Appendix (2) Guidelines for the Use of Electronic Information and Resources

AUTHORIZED ACTIVITIES	UNAUTHORIZED ACTIVITIES
▪ To use PC/MAC networking services, hardware, and software approved and/or installed on Nursing and Patient Care Services (NPCS) computers for official and authorized purposes. ▪ To use E-Mail, fax and all other information and communication services for official and authorized communication. ▪ To use application software for official and authorized purposes. ▪ To access employee data for official and authorized purposes. ▪ To use LAN computers and peripherals in the location designated for their use. ▪ To use only your password for accessing the network and other pass worded programs or documents. ▪ To use assigned personal network drive and your assigned group drive for data storage and backup. ▪ To back up all established procedures. ▪ To use enhanced telecommunication resources upon the written authorization of your supervisor and the appropriate Information Technology (IT) departments.	▪ To install, alter, modify, delete, copy, or use any additional software or hardware on the LAN without approval and Department of Networking Applications (DNA). ▪ To use insecure e-mail or fax system to transmit individually identifiable, confidential Medical Record Information. ▪ To transmit via facsimile, individually, identifiable, confidential Medical Record Information without patient consent or without being defined as "Routine Uses" by the Clinical Center Medical Records System. ▪ Use or modification of computer files or directories without proper authorization. ▪ Use or modification of computer programs, hardware, and services without proper authorization. ▪ Copying or storage of department data for other than official use. ▪ Moving or disconnecting any hardware without DNA consultation. ▪ Borrowing or using or loaning other passwords of distributing your password. ▪ Using or accessing network drives other than your assigned network drive and our assigned group drive without specific authorization. ▪ Disrupting computer or LAN services